EXHIBIT B

AO (Rev.8/97) SEARCH WARRANT ON WRITTEN AFFIDAVIT

United States District Court	DISTRICT: SOUTHERN DISTRICT OF NEW YORK
UNITED STATES OF AMERICA v. **IN THE MATTER OF THE APPLICATION OF THE UNITED STATES FOR A SEARCH WARRANT FOR THE PREMISES KNOWN AND DESCRIBED AS 110 JEWELL STREET, MAYBROOK, NEW YORK, AND CLOSED CONTAINERS AND CLOSED ITEMS CONTAINED THEREIN**	DOCKET NO. 06 MAG. 1183 / MAGISTRATE'S CASE NO. 06 MAG. 1183
	To: ANY AUTHORIZED FEDERAL AGENT

Affidavit(s) having been made before me by the below-named affiant that he/she has reason to believe that on the premises known as

110 Jewell Street, Maybrook, New York

in the Southern District of New York, there is now being concealed property, namely

SEE SCHEDULE A

and as I am satisfied that there is probable cause to believe that the property so described is being concealed on the person or premises above-described and that the grounds for application for issuance of the search warrant exist as stated in the supporting affidavit(s),

YOU ARE HEREBY COMMANDED to search on or before of _____ (not to exceed 10 days) the person or place named above for the property specified, serving this warrant and making the search (in the daytime — 6:00 A.M. to 10:00 P.M.) (At any time in the day or night)* and if the property be found there to seize it, leaving a copy of this warrant and receipt for the property taken, and prepare a written inventory of the property seized and promptly return this warrant to Any U.S. Magistrate Judge as required by law.

NAME OF AFFIANT	SIGNATURE OF JUDGE OR U.S. MAGISTRATE	DATE/TIME ISSUED
Nicholas A. Raudenski	S/MDF	1:20 PM 8/22/06

* If a search is to be authorized "at any time in the day or night" pursuant to Federal Rules of Criminal Procedure Rule 41(c), show reasonable cause therefor.

RETURN

DATE WARRANT RECEIVED	DATE AND TIME WARRANT EXECUTED	COPY OF WARRANT AND RECEIPT FOR ITEMS LEFT WITH

INVENTORY MADE IN THE PRESENCE OF

INVENTORY OF PROPERTY TAKEN PURSUANT TO THE WARRANT

CERTIFICATION

I swear that this inventory is a true and detailed account of all the property taken by me on the warrant

_____

Subscribed, sworn to, and returned before me this date.

_____ _____

Federal Judge or U.S. Magistrate *Date*

SCHEDULE A

1. Tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners in addition to computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, RM and MPEG), and the data within the aforesaid objects relating to said materials, which may be, or are, used to: visually depict child pornography; contain information pertaining to the interest in child pornography, or sexual activity with children; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography.

2. Originals and copies of photographs, negatives, magazines, motion pictures, video tapes, books, slides, audiotapes, handwritten notes, drawings and/or other visual media that depict a minor engaged in sexually explicit conduct.

3. Correspondence pertaining to the possession, receipt, distribution and/or reproduction of visual depictions of a minor engaged in sexually explicit conduct.

4. Envelopes, letters, and other correspondence, including without limitation electronic mail, chat logs, and electronic messages, identifying persons transmitting, through interstate commerce, including by computer and/or by United States Mail, any visual depiction of a minor engaged in sexually explicit conduct.

5. Books, magazines, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases or transactions of any kind involving the transmission through interstate commerce, including by computer or by United States Mail, of any visual depiction of a minor engaged in sexually explicit conduct.

6. Address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce, including by computer or by United States Mail, of any visual depiction of a minor engaged in sexually explicit conduct.

7. Address books, names and lists of names and addresses of any minor visually depicted while engaged in sexually explicit conduct.

8. Envelopes, letters, and other correspondence, including without limitation electronic mail, chat logs, and electronic messages, offering to transmit through interstate commerce, including by computer or by United States Mails, any depictions of a minor engaged in sexually explicit conduct.

9. Diaries, notebooks, notes and other records reflecting personal contact and other activities with minors visually depicted while engaged in sexually explicit conduct.

10. Materials and photographs depicting sexually explicit conduct with minors, including material that may assist in the identification and location of such minors.

11. Records evidencing ownership, tenancy, occupancy, and/or residency of the PREMISES described above.

12. Records evidencing ownership and/or use of computer equipment found in the PREMISES described above, including without limitation, sales receipts, bills for Internet access, and notes in computer manuals.

13. Records which evidence membership with any website related to child pornography, including without limitation, e-mail, correspondence and envelopes, passwords, credit card bills or receipts, and handwritten notes.

AO
(Rev.8/97)

AFFIDAVIT FOR SEARCH WARRANT

COPY

United States District Court	DISTRICT: SOUTHERN DISTRICT OF NEW YORK
UNITED STATES OF AMERICA V. IN THE MATTER OF THE APPLICATION OF THE UNITED STATES FOR A SEARCH WARRANT FOR THE PREMISES KNOWN AND DESCRIBED AS 110 JEWELL STREET, MAYBROOK, NEW YORK, AND CLOSED CONTAINERS AND CLOSED ITEMS CONTAINED THEREIN	DOCKET NO.: 06 MAGISTRATE'S CASE NO.: MAG. 118 To: Honorable Mark D. Fox United States Magistrate Judge United States Courthouse 300 Quarropas Street White Plains, New York

The undersigned being duly sworn deposes and says: That he/she has reason to believe that

☐ on the person of ☒ on the premises — DISTRICT: SOUTHERN DISTRICT OF NEW YORK

PREMISES KNOWN AND DESCRIBED AS

110 Jewell Street, Maybrook, New York and closed containers and closed items contained therein

The following property is concealed

SEE SCHEDULE A OF THE ATTACHED AFFIDAVIT

Affiant alleges the following grounds for search and seizure[2]

☒ See attached affidavit which is incorporated as part of this affidavit for search warrant

Affiant states the following facts establishing the foregoing grounds for issuance of a Search Warrant

SEE ATTACHED AFFIDAVIT

SIGNATURE OF AFFIANT	OFFICIAL TITLE, IF ANY
	Special Agent

Sworn to before me, and subscribed in my presence

DATE	JUDGE [1] OR FEDERAL MAGISTRATE

[1] United States Judge or Judge of a State Court of Record.
[2] If a search is to be authorized "at any time in the day or night" pursuant to Federal Rules of Criminal Procedure 41(c), show reasonable cause therefor

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A SEARCH WARRANT FOR THE PREMISES KNOWN AND DESCRIBED AS 110 JEWELL STREET, MAYBROOK, NEW YORK, AND CLOSED CONTAINERS AND CLOSED ITEMS CONTAINED THEREIN.	FILED UNDER SEAL AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

SOUTHERN DISTRICT OF NEW YORK, ss.:

I, NICHOLAS A. RAUDENSKI, being duly sworn, depose and say:

1. I am a Senior Special Agent of the Department of Homeland Security, U.S. Immigration and Customs Enforcement ("ICE") and have been so employed for approximately five years. I am currently assigned to a group within the New York City office of ICE that, among other things, investigates crimes against children, including the transmission of child pornography. During my tenure as a Special Agent with ICE, I have conducted and participated in numerous investigations of criminal activity, including the investigation of child pornography transmitted via computer. During the investigation of these cases, I have participated in the execution of dozens of search warrants, and have seized evidence of child pornography in connection with those search warrants.

2. I have participated in the investigation of this matter, and I am familiar with the information contained in this affidavit based on my own personal participation in the investigation, my review of documents, conversations I have had with

other law enforcement officers about this matter, my training and experience, and numerous discussions I have had with other law enforcement personnel concerning the creation, distribution, and proliferation of child pornography. Because this affidavit is being submitted for the limited purpose of establishing probable cause to search the PREMISES described below, I have not included herein the details of every aspect of the investigation. Where actions, conversations and statements of others are related herein, they are related in substance and in part, except where otherwise indicated.

3. I respectfully submit this affidavit in support of an application for a warrant to search the PREMISES described below and closed containers and closed items contained therein. Based on the facts set forth in this affidavit, there is probable cause to believe that there is presently located at the PREMISES evidence and instrumentalities of violations of federal law, including violations of Title 18, United States Code, Section 2252A. Such evidence consists of the items set forth in Schedule A to the Search Warrant.

4. I note that On August 1, 2006, the Hon. George A. Yanthis, United States Magistrate Judge, signed a search warrant authorizing a search of the PREMISES. On August 3, 2006, other law enforcement officers and I traveled to the PREMISES in an attempt to execute that search warrant. We did not execute the search warrant on that date because no one was present at the PREMISES and because a local law enforcement officer who knows the family that resides at

the PREMISES informed me that the entire family was away on vacation. We decided to wait until the family had returned from vacation before executing the search warrant. Yesterday, August 21, 2006, my supervisor was informed by a local law enforcement officer that the family that resides at the PREMISES appeared to have returned from their vacation. Since the previous search warrant expired as of August 11, 2006, I respectfully submit this affidavit in support of a new search warrant.

THE PREMISES

5. I have personally observed the area near and around 110 Jewell Street, Maybrook, New York (the "PREMISES"). The PREMISES are located at the end of Jewell Street, which is a dead-end street. The PREMISES include a two-story residence, a two-car garage, and a driveway. The ground floor of the residence has exposed brick, there is white panel siding on the second floor of the residence, and there are concrete steps leading up to the front door. Near the driveway, there is a mailbox, and a sign over the mailbox is clearly marked with the numbers "110" and "The Beebe's."

DEFINITIONS

6. The following terms have the indicated meaning in this affidavit:

a. The term "minor," "sexually explicit conduct," and "visual depiction," as used herein, are defined as set forth in Title 18, United States Code, Section 2256.

b. The term "child pornography," as used herein, is defined as set forth in Title 18, United States Code, Section 8, and means any visual depiction of a minor involved in "sexually explicit conduct" as that term is defined in Title 18, United States Code, Sections 2256(8)(A) and (C). Sections 2256(8)(A) and (C).

c. The term "computer," as used herein, is defined as set forth in Title 18, United States Code, Section 1030(e)(1).

d. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bemoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

USE OF COMPUTERS WITH CHILD PORNOGRAPHY

7. I have received training in computer crime investigation through ICE. I also use my own computer and have personal knowledge regarding the operation of computers. Based on this training, experience, and information provided to me by other law enforcement personnel involved in this investigation, I know the following:

a. The Internet is a global network which allows for the sharing of data across computers attached to the network.

b. Individual users typically access the Internet through a local Internet Service Provider ("ISP") (such as America Online) through a modem or other connection device, such as a cable or Digital Subscriber Line ("DSL"). When accessing the Internet, the ISP will assign each user an Internet Protocol ("IP") address, a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses can also be static, whereby the user's ISP assigns the computer a unique IP address, and that same number is used by the user every time the computer accesses the Internet.

c. Communication via the Internet can take place through many different mediums like accessing a website or sending and receiving electronic mail, also known and referred to herein as "e-mail." E-mail is an electronic form of communication which can contain letter-type correspondence and graphic images. E-mail is

similar to conventional paper type mail in that it is addressed from one individual to another.

d. E-mail messages usually contain a header that gives the screen name, the identity of the Internet access provider, and the return address on the Internet of the individual who originated the message or graphic.

e. The Internet also allows individuals to trade pictures or images, often through e-mail or by downloading images from a website or another individual's computer, as described below.

(1) Photographs and other images can be stored as data on a computer. This storage can be accomplished using a "scanner," which is an optical device that can recognize images or characters on paper and convert them to digital form by using specialized software.

(2) After the photograph or other image has been scanned into the computer, the computer stores the data from the image as an individual "file." Such a file is generally known as a "GIF" (Graphic Interchange Format) or "JPEG" (for the Joint Photographic Experts Group, which wrote the standard) file, recognizable by the ".gif" or ".jpg" file extensions (hereafter referred to as an "image file").

(3) Computers are capable of displaying an image file as a facsimile of the original image on a computer screen.

(4) Using a computer connected to a network connected to the Internet, one can transmit and receive image files between computers located in different states or countries.

(5) An image file itself can be either a single image (one picture only, also known as a computer file), or a multiple image file (two or more pictures, usually "zipped" or compressed using a commonly available utility and recognizable by the ".zip" file extension). Multiple image files can also be placed within an executable file (recognizable by the ".exe" file extension). When a computer runs the executable file the images can be expanded into several image files.

(6) A computer's ability to store images in digital form makes the computer an ideal repository for child pornography. Images can be stored internally in a computer on its "hard drive," externally on "floppy" disks of several sizes and capacities, or on removable media storage devices. A single floppy disk can store dozens of images and hundreds of pages of text. The storage capacities of the electronic storage media (hard drives and floppy disks) used in home computers have grown tremendously within the last several years. Hard drives with the capacity of twenty gigabytes are common. These drives can store thousands of images at a very high resolution. These images can also be stored on the computers of an Internet company hosting the particular website.

(7) With a modem, a computer user can transport an image file from the Internet or from another user's computer to his own computer, so that the image file is stored in his computer. The process of transporting an image file to one's own computer is called "downloading." The user can then display the image file on his computer screen, and can "save" or retain the images on his computer for an indefinite time period.

(8) In addition to permanently storing the downloaded image on his computer, the user may print the image file. The finished product can appear as a magazine quality picture to be stored or distributed to other collectors. The original image that was downloaded or transported is maintained in the computer.

(9) With a modem, a computer user can also send an image file that is retained in his computer to another individual or to areas of the Internet where it can be accessed by many other computer users. This process of sending an image file is called "uploading."

(10) The process of "uploading" is similar to the "downloading" process except the user is sending the computer image file to the individual or to the Internet as a whole instead of retrieving the information from another computer.

f. Another well-known component of the Internet is the World Wide Web, or the "Web." The Web is a collection of websites located or stored on different computers throughout the

world. Each website is identified by a unique Uniform Resource Locator ("URL"), which identifies the server on which the website information is stored. Users access websites by typing the corresponding URL into their web browser.

g. "Peer-to-Peer" or "File Sharing" refers to a software driven Internet network where individuals share files from their computers hard drive directly with other people over the Internet using the same software. Each user machine becomes a mini-server, as opposed to a centralized server, meaning there is no central database that knows all of the files available on the network. Instead, all of the user's machines on the network tell each other about available files using a distributed query approach.

THE INVESTIGATION

8. The information set forth below is provided as a broad overview of an investigation, named OPERATION UNDERSCORE, which led to the initial identification of Bernard Beebe as a suspected purchaser of child pornography.

9. On February 14, 2006, acting, in an undercover capacity, I entered the www.firelols.biz website ("firelols.biz"). I viewed the banner screen of the firelols.biz web site, which displayed numerous sexually explicit images depicting child pornography as defined by Title 18, United States Code, Section 2256. The firelols.biz website claimed to contain "25 GigaBytes of material inside" and "30 hours of video." I continued to tour the website, clicked on a link for "Instant Access," and was redirected to a payment web page at the URL "https://www.hpay.biz" ("hpay.biz"). The payment web page indicated that instant access could be obtained for 30 or 60 days and directed that payments be made in one of a number of forms, including the service E-Gold Ltd. ("E-Gold") - which hpay.biz described as "a very easy way to join us [the site] and keep your privacy 100% guaranteed."[1]

[1] In a nutshell, E-Gold functions as a form of electronic currency. E-Gold, so-named because the currency purchased through E-Gold is allegedly backed by actual bullion, allows individuals to use gold as money. Specifically, the E-Gold payment system enables individuals to "spend" specified weights of gold by transferring such weights of gold from one E-Gold account to another. The E-Gold payment system likewise allows

10. Upon accessing the hpay.biz website, I saw that the payment page offered customers the opportunity to use E-Gold (and other means of payment) to access any one of a total of thirteen websites (including firelols.biz). Access could be purchased for either 30-day or 60-day periods. The thirteen sites, along with the price of accessing the sites, were as follows:

Site Name	30 days access	60 days access
XL (xlola)	45.00 USD	60.00 USD
CG (candygirls)	45.00 USD	60.00 USD
ML (mylola)	100.00 USD	150.00 USD
OV (oldvideo)	100.00 USD	150.00 USD
AD (arinadreams)	100.00 USD	150.00 USD
SD (sundolls)	100.00 USD	150.00 USD
GL (goldenlols)	100.00 USD	150.00 USD
FL (firelols)	100.00 USD	150.00 USD
LO (lolsonly)	100.00 USD	150.00 USD
HL (hotlols)	100.00 USD	150.00 USD
A2 (arinadreams II)	200.00 USD	400.00 USD
LH (lolhouse)	150.00 USD	
SA (secret area)	200.00 USD (only for members of LH)	
LH + SA (lolhouse + secret area)	350.00 USD	

The payment page also prompted customers to provide an e-mail address at which customers could receive login & password information for instant access to one or more of these thirteen websites.

11. The website also had a preview page,

---

payments to be made in terms of actual currencies. Thus, for example, it is possible to spend $100.00 worth of e-gold.

Customers can deposit funds into their E-Gold accounts by charging an amount to their credit cards or by submitting an alternate form of payment such as a money order. Customers can debit their accounts by transferring funds to other E-Gold accounts.

"http://www.lolsites.info/preview/", at which customers were given the opportunity to download free previews of all of the thirteen sites listed at hpay.biz. These free previews included free video and picture/image files.

12. On February 15, 2006, law enforcement officers working with ICE downloaded files from the free previews for twelve of the thirteen websites listed on hpay.biz. Law enforcement officers subsequently downloaded files from the free preview for the thirteenth website, "SD" (Sundolls site) on April 26, 2006. All the files downloaded from the free previews for the thirteen websites exclusively contained images of child pornography as defined by Title 18, United States Code, Section 2256. And all the websites had advertised that the images contained in the free previews were indicative of the material that would be found in the websites, themselves.

13. Following an initial investigation in the Eastern District of New York, on or about March 1, 2006, another ICE agent ("Undercover #1) and I sent separate e-mail messages from separate undercover e-mail addresses to the customer support offered at the "xlola.biz" site. That website had indicated that "You can write to us if you have any problems and any questions. We will answer you shortly! Our support email is <support@xlola.biz>." In each email, an undercover agent alleged that he or she had had problems signing up for the websites and requested that xlola.biz email back the

number of an E-Gold account into which funds could be deposited in order to gain access to the web sites.

14. On March 1, 2006, Undercover # 1 received a response from "Support@xlola.biz" stating that he was "welcome to transfer money directly" to E-Gold account number 2932763. Two days later, on March 3, 2006, I received a similar response from Support@xlola.biz, but I was directed to transfer money directly to E-Gold account number 2928629.

15. On March 6, 2006, another ICE agent working in an undercover capacity purchased a membership to the child pornography website identified as "www.firelols.biz." The agent observed that the website contained images of child pornography in video format only. Over a period of days, an ICE agent downloaded all of the material available from firelols.biz, confirming that the site entirely and exclusively contained child pornography as defined by Title 18, United States Code, Section 2256.

16. On March 7, 2006, ICE issued a summons to E-Gold Ltd. ("E-Gold"), for records related to E-Gold accounts 2932763 and 2928629 as well as any account identified to be related to these accounts. Specifically, ICE directed E-Gold to provide, inter alia, account profiles and transaction histories for all subscribers who had transferred money into either E-Gold account 2932763 or E-Gold account 2928629. On March 10, 2006, E-Gold provided the account profiles and transaction histories for all of the subscribers as well

as the web sites' E-gold accounts for a period from January 5, 2006 through March 9, 2006. Approximately 150 subscribers nationwide and worldwide were identified as having purchased access to these web sites in the defined time period. One of the subscribers was an individual who had given, among other information, the name Bernard Beebe, the address 110 Jewell Street, Maybrook, New York, and the email address dbeebe1@hvc.rr.com. This information was associated with E-Gold account number 2808925.

17. Based on my review of the information provided by E-Gold, I know that Beebe held E-Gold account # 2808925 and, through that account, purchased access to three (3) web sites identified as "CandyGirls", "XLola" and "LolHouse" within the "www.lolsites.biz," group of child pornography sites. On February 11, 2006, Beebe paid $45 to access the "CandyGirls" website for 30 days; that same date, Beebe paid $45 to access the "XLola" website for 30 days; and subsequently on February 25, 2006, Beebe paid $150 to access "LolHouse" for 30 days.

18. On March 14, 2006 and again on May 30, 2006, ICE Agents conducted drive by surveillance on the PREMISES. Agents observed a 2003 Green Ford Econoline 350 Van with New York license plate number AJY-8578 parked on the street in front of the PREMISES. This vehicle is registered to Bernard J. Beebe (Date of Birth: 04/11/1960) at 110 Jewel Street, Maybrook, NY 12543 which is the PREMISES.

19. A query of a certain commercial database provided that Bernard J. Beebe (DOB: 04/11/1960; SSN: 063-56-4935) resided at 110 Jewell St., Maybrook, NY 12543.

20. On June 2, 2006, Time Warner Cable provided account information for the individuals living at 110 Jewell Street in Maybrook, New York. The individuals were BJ and Deborah Beebe and their user ID's were "dbeebe1@hvc.rr.com" and "bbeebe1@hvc.rr.com." Time Warner Cable further indicated that the account associated with the email address "dbeebe1@hvc.rr.com" was activated on January 6, 2006 and remained active as of June 2, 2006.

USE OF THE INTERNET AND COMPUTERS FOR CHILD PORNOGRAPHY

21. Based on my training, experience and conversations with other law enforcement agents, I know that computers, computer technology and the Internet have revolutionized the way in which child pornography is produced, distributed, utilized and collected. They have revolutionized also the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were significant costs involved with the production of pornographic images. To distribute these images on any scale also

required significant resources. The photographs were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

22. The development of computers and the Internet has added to the methods used by child pornography collectors to interact with and sexually exploit children and to produce and distribute child pornography. Computers and the Internet generally serve four functions in connection with child pornography. These are: production, communication, distribution, and storage.

a. Child pornographers now can produce both still and moving images directly from a common video camera. The captured images can be edited in very similar ways to a photograph. The image can be lightened, darkened, cropped, and manipulated in a wide variety of ways. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. Further, it is more difficult for law enforcement to detect and investigate child pornography produced with this new technology, as opposed to methods used in the past, which required more elaborate and detectable equipment and facilities, as described above in paragraph 18.

b. Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade or market pornography. The development of computer technology has changed that. A modem allows any computer to connect to another computer through the use of telephone lines. By connecting to a host computer, electronic contact can be made to numerous other computers around the world. Once this electronic contact is established, there are numerous outlets and ways that child pornography can be distributed over the Internet.

c. Private and/or public Internet relay chat ("IRC") channels can be and are created for the purpose of sharing child pornography. A user can log onto the IRC anonymously and "chat" and/or trade child pornography with other users, either on an individual or group basis. During this type of session no identifying personal information is obvious or available. The only identifiable or traceable information is the individual's IP address and ISP. IRC chatrooms are one place where pornographers meet to trade child related sexual and non-sexual stories and trade child pornography. It is also a place where children may be at risk of being "lured."

d. Aside from "chat rooms" that reside on many service providers' networks, ISPs often allow access to "newsgroups." Newsgroups resemble a bulletin board system where an individual can post messages along with graphic files on a public forum. Any item

posted in a news group can be retrieved by any other person who has access to that particular newsgroup. One commonality between a newsgroup posting and e-mail is that they each often contain a message "header" that gives information about the account that originated a particular message and/or graphic files, and the return address to respond to the poster/sender.

e. Internet websites also can be used to facilitate the exchange of child pornography. A website can house child pornography directly, allowing users who access the website to view and download those images. A website can also house an "Egroup," which is a forum by which persons with shared interests in child pornography can interact in relative privacy. Typically, most Egroups will have a moderator, and membership in the group can be open or by invitation only. The members of an Egroup also typically communicate with each other by sending an e-mail to the group, which is disseminated to all of the members. In addition, each Egroup typically has a web page that the group's members can visit to view archived postings. E-mail messages and postings might include files that contain visual depictions and digital video clips.

f. These communication structures are ideal for the child pornography collector. The open and anonymous communication allows the user to locate others of similar inclination and still maintain anonymity. Once contact has been established, it is possible to send text messages and graphic images to others.

Moreover, the child pornography collector need not use the large service providers. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages are well known and are the foundation of transactions between child pornography collectors.

g. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution of child pornography. For example, child pornography can be transferred (via electronic mail, through file transfer protocols[2] ("FTPs"), or via newsgroup postings) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services, and easy access to the Internet, the computer is a preferred method of distribution of child pornographic materials.

---

[2] The File Transfer Protocol ("FTP") is a protocol that defines how to transfer files from one computer to another. One use, known as "anonymous FTP," allows users who do not have a login name or password to access certain files from another computer, and copy those files to their own computer.

h. The computer's capability to store images in digital form makes it an ideal repository for pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 20 gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Further, magnetic storage located in host computers allows child pornographers to hide pornographic images from law enforcement. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and to save that image to storage on a host computer in another country. Only careful laboratory examination of electronic storage devices can recreate the evidence trail.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

23. Based on my training and experience as a Special Agent of ICE and conversations that I have had with other federal agents and law enforcement officers, I know that child pornography is not readily available in retail establishments. Accordingly, individuals who wish to obtain child pornography do so usually by ordering it from abroad or by discreet contact, including through the use of the Internet, with other individuals who have it available or by accessing web sites containing child pornography. Child pornography

collectors often send and receive electronic mail conversing with other collectors in order to solicit and receive child pornography.

24. I know that child pornography collectors usually maintain and possess their materials (computer images, pictures, films, magazines, videotapes, correspondence, source information, etc.) in a private secure location such as their home, office, or work space. Images or videos taken off of the Internet are often stored in the hard drive of the computer or on diskettes kept in private locations near the computer such as in locked desks, shelves, contiguous work space, filing cabinets or similar items and areas in office space. These images also can be printed on computer printers and maintained by child pornography collectors in paper form. Additionally, child pornography collectors often transfer those images to videotape, either by videotaping with a handheld video camera the images or videos on a computer screen, or by connecting a video cassette recorder to the computer and recording the images or videos directly.

25. Collectors of child pornography typically retain their materials and related information for many years. Most collectors of child pornography seek to increase the size of their collections in a manner similar to collectors of coins, stamps, or rare books. Many retain these materials, including information regarding sources, for their entire adult lives. Moreover, individuals who distribute and/or collect child pornography generally prefer not to be without

their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. In addition, collectors of child pornography rarely destroy correspondence from other collectors or distributors unless their activities are uncovered by law enforcement authorities or others.

26. Accordingly, information in support of probable cause in child pornography cases is less likely to be stale because collectors and traders of child pornography are known to store and retain their collections for extended periods of time, usually in their home. Indeed, as noted above, based on my experience with child pornography search warrants, I know that even where information about a suspect's use of child pornography is not current, we typically find child pornography at the location of the search, assuming the suspect still resides there.

27. Additionally, based on my experience and training, I know that persons who collect and distribute child pornography:

a. Frequently collect sexually explicit materials in a variety of media, such as photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media that they use for their own sexual arousal and gratification. Further, they commonly use this type of sexually explicit material to lower the inhibitions of children they are attempting to seduce, to arouse

the selected child partner, and to demonstrate the desired sexual acts.

b. Frequently receive sexual gratification, stimulation, and satisfaction from actual physical contact with children and/or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses (in person, in photographs, or other visual media) or from literature describing such activity.

c. Often correspond and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, telephone numbers and screen names of individuals with whom they have been in contact and who share the same interests in child pornography.

28. Based on my training and experience and my conversations with other members of ICE, I have also learned that:

a. Child pornography is a permanent record of the sexual abuse of a child victim. Each time child pornography is reproduced, downloaded, or forwarded by an Internet user, the victimization of the minor appearing in the pornography is perpetuated. Such items also are important evidence and indications of an individual whose sexual objects are children, and of that individual's motive, intent, and predisposition to violate federal

law related to the distribution of child pornography. Additionally, these items lead to the identification of child victims and other individuals engaging in similar conduct.

b. Child pornography collectors reinforce their fantasies, often by taking progressive, overt steps aimed at turning the fantasy into reality in some or all of the following ways: collecting and organizing their child-related material; masturbating while viewing the child pornography; engaging children, online and elsewhere, in conversations, sometimes sexually explicit conversations, to fuel and fortify the fantasy; interacting, both directly and indirectly, with other like-minded adults through membership in organizations catering to their sexual preference for children thereby providing a sense of acceptance and validation within a community; gravitating to employment, activities and/or relationships which provide access or proximity to children; and frequently persisting in the criminal conduct even when they have reason to believe the conduct has come to the attention of law enforcement. These are need driven behaviors to which the offender is willing to devote considerable time, money, and energy in spite of risks and against self interest. The "collection" is the best indicator that law enforcement has of what the collector wants to do, not necessarily what he has done or will do. The overriding motivation for the collection of child pornography may be to define,

fuel, and validate the collectors most cherished sexual fantasies involving children.

REQUEST TO SEARCH THE PREMISES

29. In light of the foregoing information, and based on my experience and training, I submit that there is probable cause to believe that the PREMISES contain child pornography or other evidence concerning violations of Title 18, United States Code, Section 2251(C), publishing a notice or advertisement seeking or offering to exchange child pornography, and that the fruits and instrumentalities of those violations can be found at the PREMISES. Specifically, any computers or computer equipment at the PREMISES are likely to be the primary means of accessing the Internet for purposes of distributing or collecting child pornography and therefore may be seized "as the means of committing [the] criminal offense" pursuant to Federal Rule of Criminal Procedure 41(b)(3). The evidence, fruits, and instrumentalities of the offenses include the items described in Schedule A, attached.

METHODS TO BE USED TO SEIZE AND SEARCH COMPUTERS AND COMPUTER-RELATED EQUIPMENT

30. Based upon my training, experience, and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know that searching computerized information for evidence or

instrumentalities of a crime commonly requires agents to seize most or all of a computer system's input/output peripheral devices, related software documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true for the following reasons:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

b. Searching computer systems requires the use of precise, scientific procedures that are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Because computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a

complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. Typically, the volume of data stored on many computer systems and storage devices will be so large that it would be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing up to 40 gigabytes of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of millions of pages of data.

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography."

For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

31. In searching for data capable of being read, stored or interpreted by a computer, law enforcement personnel executing this search warrant will employ the following procedure:

a. Upon securing the premises, law enforcement personnel trained in searching and seizing computer data (the "computer personnel") will make an initial review of any computer equipment and storage devices to determine whether these items contain contraband and whether these items can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve the data.

b. If the computer equipment and storage devices cannot be searched on-site within a reasonable amount of time and without jeopardizing the ability to preserve the data, and if the computer equipment and storage devices do not contain contraband, then the computer personnel will determine whether it is practical to copy the data during the execution of the search in a reasonable amount of time without jeopardizing the ability to preserve the data.

c. If the computer personnel determine that these items contain contraband, or that it is not practical to perform an on-site search or make an on-site copy of the data, then the computer equipment and storage devices will be seized and transported to an appropriate law enforcement laboratory for review. The computer equipment and storage devices will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized set forth herein.

d. The analysis of electronically stored data, whether performed on-site or in a separate, controlled environment, may entail any or all of several different techniques. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); "opening" or reading the first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "key-word" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

32. Any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offense, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offense specified above.

33. In searching the data, the computer personnel may examine all of the data contained in the computer equipment and storage devices to view their precise contents and determine whether the data falls within the items to be seized as set forth herein. In addition, the computer personnel may search for and attempt to recover "deleted," "hidden" or encrypted data to determine whether the data falls within the list of items to be seized as set forth herein.

34. If the computer personnel determine that the computer equipment and storage devices are no longer necessary to retrieve and preserve the data, and the items are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(b), the government will return these items, upon request, within a reasonable period of time.

35. In order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize and search the following items, subject to the procedures set forth above:

a. Any computer equipment and storage device capable of being used to commit, further or store evidence of the offense listed above;

b. Any computer equipment used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners;

c. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the computer equipment, storage devices or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices or data to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

****

Based on the foregoing, I believe there is probable cause to believe that a search of the PREMISES will lead to the discovery of the items set forth in Schedule A. The search warrant, if issued, will be executed during the day time as defined in Fed. R. Crim. P. 41(e)(2)(B), within 10 days of the date of the issuance of the warrant as required by Fed. R. Crim. P. 41(e)(2)(A).

I also respectfully request that the court issue an Order pursuant to which the Application and Affidavit for the search warrant be filed under seal. The information contained in these materials is relevant to an ongoing investigation and premature disclosure of the Application and Affidavit for the search warrant would substantially jeopardize the effectiveness of the investigation.

Additionally, I affirm that any computers or computer-related material seized from the PREMISES will be returned within 60 days of the execution of the Search Warrant, unless, upon a motion from the Government, the Court issues an order to the contrary.

WHEREFORE, I respectfully request that the Search Warrant sought herein issue pursuant to Rule 41 of the Federal Rules of Criminal Procedure, permitting authorized agents or officers to enter the PREMISES and therein to search for and seize the items listed in Schedule A to the Search Warrant.

SPECIAL AGENT NICHOLAS A. RAUDENSKI
BUREAU OF IMMIGRATION AND
CUSTOMS ENFORCEMENT

Sworn to before me this
22nd day of August 2006

UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK